(4) A description of control or monitoring system connections to non-vital systems.

(5) A description of programable features.

(6) A description of built-in test features and diagnostics.

(7) Design Verification and Periodic Safety test procedures described in subpart 61.40 of this chapter.

(8) Control system normal and emergency operating instructions.

§ 62.20–3 Plans for information.

(a) One copy of the following plans must be submitted to the Officer in Charge, Marine Inspection, for use in the evaluation of automated systems provided to replace specific personnel or to reduce overall crew requirements:

(1) Proposed manning, crew organization and utilization, including routine maintenance, all operational evolutions, and emergencies.

(2) A planned maintenance program for all vital systems.

(b) One copy of a qualitative failure analysis must be submitted in accordance with §50.20–5 of this chapter for the following:

(1) Propulsion controls.

(2) Microprocessor-based system hardware.

(3) Safety controls.

(4) Automated electric power management.

(5) Automation required to be independent that is not physically separate.

(6) Any other automation that, in the judgement of the Commandant, potentially constitutes a safety hazard to the vessel or personnel in case of failure.

NOTE: The qualitative failure analysis is intended to assist in evaluating the safety and reliability of the design. It should be conducted to a level of detail necessary to demonstrate compliance with applicable requirements and should follow standard qualitative analysis procedures. Assumptions, operating conditions considered, failures considered, cause and effect relationships, how failures are detected by the crew, alternatives available to the crew, and possible design verification tests necessary should be included. Questions regarding failure analysis should be referred to the Marine Safety Center at an early stage of design.

§ 62.20–5 Self-certification.

(a) The designer or manufacturer of an automated system shall certify to the Coast Guard, in writing, that the automation is designed to meet the environmental design standards of §62.25–30. Plan review, shipboard testing, or independent testing to these standards is not required.

(b) [Reserved]

NOTE: Self-certification should normally accompany plan submittal.

Subpart 62.25—General Requirements for All Automated Vital Systems

§ 62.25–1 General.

(a) Vital systems that are automatically or remotely controlled must be provided with—

(1) An effective primary control system;

(2) A manual alternate control system;

(3) A safety control system, if required by §62.25–15;

(4) Instrumentation to monitor system parameters necessary for the safe and effective operation of the system; and

(5) An alarm system if instrumentation is not continuously monitored or is inappropriate for detection of a failure or unsafe condition.

(b) Automation systems or subsystems that control or monitor more than one safety control, interlock, or operating sequence must perform all assigned tasks continuously, i.e., the detection of unsafe conditions must not prevent control or monitoring of other conditions.

(c) Vital control and alarm system consoles and similar enclosures that rely upon forced cooling for proper system operation must meet section 41.23.2 of the American Bureau of Shipping's ''Rules for Building and Classing Steel Vessels.''

§ 62.25–5 All control systems.

(a) Controls for engines and turbines equipped with jacking or turning gear must meet section 41.21.4 of the American Bureau of Shipping's ''Rules for Building and Classing Steel Vessels.''

(b) Automatic control systems must be stable over the entire range of normal operation.

(c) Inadvertent grounding of an electrical or electronic safety control system must not cause safety control operation or safety control bypassing.

§ 62.25–10 Manual alternate control systems.

(a) Manual alternate control systems must—

(1) Be operable in an emergency and after a remote or automatic primary control system failure;

(2) Be suitable for manual control for prolonged periods;

(3) Be readily accessible and operable; and

(4) Include means to override automatic controls and interlocks, as applicable.

(b) Permanent communications must be provided between primary remote control locations and manual alternate control locations if operator attendance is necessary to maintain safe alternate control.

NOTE: Typically, this includes main boiler fronts and local propulsion control.

§ 62.25–15 Safety control systems.

(a) Minimum safety trip controls required for specific types of automated vital systems are listed in Table 62.35–50.

NOTE: Safety control systems include automatic and manual safety trip controls and automatic safety limit controls.

(b) Safety trip controls must not operate as a result of failure of the normal electrical power source unless it is determined to be the failsafe state.

(c) Automatic operation of a safety control must be alarmed in the machinery spaces and at the cognizant remote control location.

(d) Local manual safety trip controls must be provided for all main boilers, turbines, and internal combustion engines.

(e) Automatic safety trip control systems must—

(1) Be provided where there is an immediate danger that a failure will result in serious damage, complete breakdown, fire, or explosion;

(2) Require manual reset prior to renewed operation of the equipment; and

(3) Not be provided if safety limit controls provide a safe alternative and trip would result in loss of propulsion.

§ 62.25–20 Instrumentation, alarms, and centralized stations.

(a) *General.* Minimum instrumentation and alarms required for specific types of automated vital systems are listed in Table 62.35–50.

(b) *Instrumentation Location.* (1) Manual control locations, including remote manual control and manual alternate control, must be provided with the instrumentation necessary for safe operation from that location.

NOTE: Typically, instrumentation includes means to monitor the output of the monitored system.

(2) Systems with remote instrumentation must have provisions for the installation of instrumentation at the monitored system equipment.

(3) The status of automatically or remotely controlled vital auxiliaries, power sources, switches, and valves must be visually indicated in the machinery spaces or the cognizant remote control location, as applicable.

NOTE: Status indicators include run, standby, off, open, closed, tripped, and on, as applicable. Status indicators at remote control locations other than the ECC, if provided, may be summarized. Equipment normally provided with status indicators are addressed in Table 62.35–50 and subparts 58.01, 56.50, and 112.45.

(4) Sequential interlocks provided in control systems to ensure safe operation, such as boiler programing control or reversing of propulsion diesels, must have summary indicators in the machinery spaces and at the cognizant control location to show if the interlocks are satisfied.

(5) Instrumentation listed in Table 62.35–50 must be of the continuous display type or the demand display type. Displays must be in the ECC or in the machinery spaces if an ECC is not provided.

(c) *Instrumentation details.* Demand instrumentation displays must be clearly readable and immediately available to the operator.